UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,477	07/14/2004	James E. Aston	014682.000010	4476

44870 7590 06/06/2007

MOORE & VAN ALLEN, PLLC For IBM
P.O. Box 13706
Research Triangle Park, NC 27709

EXAMINER	
DWIVEDI, MAHESH H	
ART UNIT	**PAPER NUMBER**
2168	
MAIL DATE	**DELIVERY MODE**
06/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/710,477	ASTON ET AL.	
	Examiner	Art Unit	
	Mahesh H. Dwivedi	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07/14/2004* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/02/2006 has been entered.

Remarks

2. Receipt of Applicant's Amendment filed on 03/12/2007 is acknowledged. The amendment includes amending claims 1-2, 9, 21, and 30, and the cancellation of claim 6.

Claim Objections

3. Claim 20 is objected to because of the following informalities: The phrase "operations **associated the program**" should be changed to "operations **associated with the program**". Appropriate correction is required.

Claim 28 is objected to because of the following informalities: The phrase "in response to the **program other being**" should be changed to "in response to the **other program being**". Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1, 9, 21, 30, and 38 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Specifically, the examiner wishes to state that the amended limitation of "**without performing any virus scanning**

and detection actions" is not adequately defined nor explained in any detail as to how the instant application accomplishes virus detection without performing active actions. The examiner requests that applicant specifically point out in the specification of the instant application where the aforementioned limitation is described.

Claims 2-5, 7-8, 10-20, 22-29, 31-37, and 39-44 are rejected for incorporating the deficiencies of independent claims 1, 9, 21, 30, and 38.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1, 9, 21, 30, and 38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the examiner wishes to state that the amendment of "without performing any virus scanning and detection actions" is vague, indefinite, and contradictory to the rest of the limitations of the independent claims. Moreover, the examiner wishes to state that the limitations of the independent claims clearly point to the fact that since monitoring operations of a computer system are primarily involved in the detection of potential viruses in the instant application, then the instant application is in fact performing virus detection and scanning actions.

Claims 2-5, 7-8, 10-20, 22-29, 31-37, and 39-44 are rejected for incorporating the deficiencies of independent claims 1, 9, 21, 30, and 38.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 21-29 are rejected under 35 U.S.C. 101 as being directed non-statutory subject matter. The language of the claim raises a question as to whether the claim is directed merely to an environment or machine which would result in a practical application producing a concrete useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Software or program can be stored on a medium and/or executed by a computer. In other words, software must be computer readable. The use of computer is not evident in these claims.

10. **For your reference, below is a section from MPEP 2105 :**

(a) Functional Descriptive Material: "Data Structures" Representing Descriptive Material Per Se or Computer Programs Representing Computer Listings Per Se Data structures not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a data structure defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory. Similarly, computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. Accordingly, it is important to distinguish claims that

define descriptive material per se from claims that define statutory inventions. Computer programs are often recited as part of a claim. Office personnel should determine whether the computer program is being claimed as part of a otherwise statutory manufacture or machine. In such a case, the claim remains statutory irrespective of the fact that a computer program is included in the claim. The same result occurs when a computer program is used in a computerized process where the computer executes the instructions set forth in the Computer program. Only when the claimed invention taken as a whole is directed to a mere program listing, i.e., to only its description or expression, is it descriptive material per se and hence nonstatutory.

Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and Office personnel should treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material. When a computer program is claimed in a process where the computer is executing the computer program's instructions, Office personnel should treat the claim as a process claim. See paragraph IV.B.2(b), below. When a computer program is recited in conjunction with a physical structure, such as a computer memory, Office personnel should treat the claim as a product claim.

11. Claims 38-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 62-68 appear to represent nonfunctional descriptive material. Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support

specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a computer-readable medium, in a computer, on an electromagnetic carrier signal does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer."). Such a result would exalt form over substance. See also In re Johnson, 589 F.2d 1070, 1077, 200 USPQ 199, 206 (CCPA 1978) ("form of the claim is often an exercise in drafting"). Thus, nonstatutory music is not a computer component and it does not become statutory by merely recording it on a compact disk. Protection for this type of work is provided under the copyright law.

Claims 38-44 are further rejected under 35 U.S.C 101 because the claimed invention is directed to the non-statutory subject area of electro-magnetic signals, carrier waves. Claims 38-44 recite the limitation **"computer-readable medium"**. The examiner interprets "computer-readable medium" as a computer-readable medium defined by the characteristics in paragraph 28 of the applicant's specification. According to paragraph 28 of the applicant's specification, a computer-readable medium may access "The I/O devices 248 may also include disk drives, optical, mechanical, magnetic, or **infrared** input/output devices, modems or the like. The I/O devices may be used to access a medium 252. The medium 252 may contain, store, communicate or transport computer-readable or computer executable instructions or other information for use by or in connection with a system, such as the computer system 214"

(Paragraph 28). Claims 38-44 recite nothing but the physical characteristics of a form of energy, such as a frequency, voltage, or the strength of a magnetic field, define energy or magnetism, per se, and as such are nonstatutory natural phenomena. O'Reilly, 56 U.S. (15 How.) at 112-14. Moreover, a claim reciting a signal encoded with functional descriptive material does not fall within any of the categories of patentable subject matter set forth in § 101. First, a claimed signal is clearly not a "process" under § 101 because it is not a series of steps. The other three § 101 classes of machine, compositions of matter and manufactures "relate to structural entities and can be grouped as 'product' claims in order to contrast them with process claims." 1 D. Chisum, Patents § 1.02 (1994). The three product classes have traditionally required physical structure or material. "The term machine includes every mechanical device or combination of mechanical device or combination of mechanical powers and devices to perform some function and produce a certain effect or result." Corning v. Burden, 56 U.S. (15 How.) 252, 267 (1854). A modern definition of machine would no doubt include electronic devices which perform functions. Indeed, devices such as flip-flops and computers are referred to in computer science as sequential machines. A claimed signal has no physical structure, does not itself perform any useful, concrete and tangible result and, thus, does not fit within the definition of a machine. A "composition of matter" "covers all compositions of two or more substances and includes all composite articles, whether they be results of chemical union, or of mechanical mixture, or whether they be gases, fluids, powders or solids." Shell Development Co. v. Watson, 149 F. Supp. 279, 280, 113 USPQ 265, 266 (D.D.C. 1957), aff'd, 252 F.2d 861, 116 USPQ 428 (D.C. Cir. 1958). A claimed signal is not matter, but a form of energy, and therefore is not a composition of matter. The Supreme Court has read the term "manufacture" in accordance with its dictionary definition to mean "the production of articles for use from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by hand-labor or by machinery." Diamond v. Chakrabarty, 447 U.S. 303, 308, 206 USPQ 193, 196-97 (1980)

(quoting American Fruit Growers, Inc. v. Brogdex Co., 283 U.S. 1, 11, 8 USPQ 131, 133 (1931), which, in turn, quotes the Century Dictionary). Other courts have applied similar definitions. See American Disappearing Bed Co. v. Arnaelsteen, 182 F. 324, 325 (9th Cir. 1910), cert. denied, 220 U.S. 622 (1911). These definitions require physical substance, which a claimed signal does not have. Congress can be presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. Lorillard v. Pons, 434 U.S. 575, 580 (1978). Thus, Congress must be presumed to have been aware of the interpretation of manufacture in American Fruit Growers when it passed the 1952 Patent Act. A manufacture is also defined as the residual class of product. 1 Chisum, § 1.02[3] (citing W. Robinson, The Law of Patents for Useful Inventions 270 (1890)). A product is a tangible physical article or object, some form of matter, which a signal is not. That the other two product classes, machine and composition of matter, require physical matter is evidence that a manufacture was also intended to require physical matter. A signal, a form of energy, does not fall within either of the two definitions of manufacture. Thus, a signal does not fall within one of the four statutory classes of § 101.

To expedite a complete examination of the instant application, the claims rejected under 35 U.S.C. 101 (nonstatutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four categories of invention.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1-2, 5, 7-9, 12-19, 21-30, 32-38, and 40-44 are rejected under 35 U.S.C. 102(b) as being anticipated by **Halperin et al.** (U.S. PGPUB 2002/0194490).

14. Regarding claim 1, **Halperin** teaches a method comprising:

A) flagging a program as being suspect for possibly containing a virus without performing any virus scanning and detections actions in response to at least one of: opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set (Abstract, Paragraphs 73-77, and 88-108);

B) storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program without performing any virus scanning and detection actions (Paragraphs 108).

The examiner notes that **Halperin** teaches **"flagging a program as being suspect for possibly containing a virus without performing any virus scanning and detections actions in response to at least one of: opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of**

the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system and at least the medium security level being set" as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **"storing a filename and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the program without performing any virus scanning and detection actions"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The

server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 2, **Halperin** further teach a method comprising:
A) inhibiting a write or append operation associated with program in response to flagging the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"inhibiting a write or append operation associated with program in response to flagging the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may

be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 5, **Halperin** further teaches a method comprising:

A) sending an alert in response to flagging the program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to flagging the program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 7, **Halperin** further teaches a method comprising:

A) sending an alert to a network monitoring system in response to flagging the program (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending an alert to a network monitoring system in response to flagging the program"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 8, **Halperin** further teaches a method comprising:

A) logging any file system operations including recording a filename and a location where the local or shared file is written (Paragraph 108).

The examiner notes that **Halperin** teaches **"logging any file system operations including recording a filename and a location where the local or shared file is written"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 9, **Halperin** teaches a method comprising:

A) allowing a security level to be set (Paragraphs 43-44, 108, and 111);

B) monitoring predetermined file system operations associated with a program (Abstract, Paragraphs 73-77, and 88-108); and

C) logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written without performing any virus scanning and detection actions (Paragraphs 108).

The examiner notes that **Halperin** teaches **"allowing a security level to be set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"monitoring predetermined file system operations associated with a program"** "Reference is now made to FIG. 6, which is a simplified flowchart

illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and " Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written without performing any virus scanning and detection actions"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay

period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 12, **Halperin** further teaches a method comprising:
A) receiving a notification that the program intends to perform one of the predetermined file system operations (Paragraph 108).

The examiner notes that **Halperin** teaches **"receiving a notification that the program intends to perform one of the predetermined file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for

messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 13, **Halperin** further teaches a method comprising:
A) following a predefined procedure in response to the level of security set (Paragraphs 43-44, 108, and 111).

The examiner notes that **Halperin** teaches **"following a predefined procedure in response to the level of security set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown

virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 14, **Halperin** further teaches a method comprising:
A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 15, **Halperin** further teaches a method comprising:
A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether

the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 16, **Halperin** further teach a method comprising:
A) inhibiting any predetermined file system operations associated with program in response to the program being flagged (Paragraph 108).

The examiner notes that **Halperin** teaches **"inhibiting any predetermined file system operations associated with program in response to the program being flagged"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe,

.doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 17, **Halperin** further teaches a method comprising:
A) sending an alert in response to the program attempting to perform any predetermined file system operations (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 18, **Halperin** further teaches a method comprising:
A) sending the alert to a network monitoring system (Paragraph 111).

The examiner notes that **Halperin** teaches **"sending the alert to a network monitoring system"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 19, **Halperin** further teaches a method comprising:
A) presenting an alert to a user for approval before the predetermined file system operation is performed by the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"presenting an alert to a user for approval before the predetermined file system operation is performed by the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Regarding claim 21, **Halperin** teaches a system comprising:

A) a file system protection program including: means to monitor predetermined file system operations associated with another program (Abstract, Paragraphs 73-77, and 88-108);

B) a plurality of settable levels of security (Paragraphs 43-44, 108, and 111);

C) a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security (Paragraphs 43-44, 108, and 111); and

D) means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written without performing any virus scanning and detection actions (Paragraph 108).

The examiner notes that **Halperin** teaches **"a file system protection program including: means to monitor predetermined file system operations associated with another program"** "Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of

operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and " Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches **"a plurality of settable levels of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users,

different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired

levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written without performing any virus scanning and detection actions"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be

applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 23, **Halperin** further teaches a system comprising:
A) a log to record any predetermined file system operations (Paragraphs 108 and 131).

The examiner notes that **Halperin** teaches **"a log to record any predetermined file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108) and "The present invention may be used to identify suspicious activity as it begins to spread within a first group and then receive a report of similar suspicious activity in a second

group that is not a neighbor of the first group. In this case, the present invention may be used to analyze recent log files of communications between computing devices in the first and second groups. Since the groups are not neighbors, such communications are not likely to be found under normal circumstances. If a recent communication is identified between the two groups, this may be treated as a suspicious event. The communication may then be forwarded to a human operator for analysis to identify malicious software. In addition, this process may be used to identify the specific communication message that is carrying the virus, which may lead to containment actions being taken" (Paragraph 131).

Regarding claim 24, **Halperin** further teaches a system comprising:
A) means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other**

program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system" as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 25, **Halperin** further teaches a system comprising:
A) means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations"** as "A method for malicious software

detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 26, **Halperin** further teaches a system comprising:
A) means to send an alert in response to flagging the other program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"means to send an alert in response to flagging the other program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 27, **Halperin** further teaches a system comprising:
A) a network monitoring system (Paragraph 111); and

B) means to send an alert to the network monitoring system in response to flagging the other program (Paragraph 111)

The examiner notes that **Halperin** teaches **"a network monitoring system"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"means to send an alert to the network monitoring system in response to flagging the other program"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 28, **Halperin** further teach a system comprising:
A) means to inhibit predetermined file system operations associated with the other program in response to the program other being flagged (Paragraph 108).

The examiner notes that **Halperin** teaches **"means to inhibit predetermined file system operations associated with the other program in response to the program other being flagged"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The

server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 29, **Halperin** further teaches a system comprising:
A) means to present an alert to a user (Paragraphs 73-77); and
B) means for the user to approve one of the predetermined file system operations before being performed by the other program (Paragraph 108).

The examiner notes that **Halperin** teaches **"means to send an alert in response to flagging the other program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **"means for the user to approve one of the predetermined file system operations before being performed by the other program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from

reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Regarding claim 30, **Halperin** teaches a method comprising:
A) providing means to monitor predetermined file system operations associated with another program (Abstract, Paragraphs 73-77, and 88-108);
B) defining a plurality of settable levels of security (Paragraphs 43-44, 108, and 111);
C) providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security (Paragraphs 43-44, 108, and 111); and
D) providing means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written without performing any virus scanning and detection actions (Paragraph 108).

The examiner notes that **Halperin** teaches **"providing means to monitor predetermined file system operations associated with another program"** "Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and " Any

known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that **Halperin** teaches **"defining a plurality of settable levels of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such

diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"providing a predefined procedure associated with each level of security to be followed in response to a current level of security being set for the predefined procedure and in response to an intent to perform a particular file system operation also associated with the currently set level of security"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system

decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"providing means to log any predetermined file system operations associated with the other program including recording a filename and location where a file is written without performing any virus scanning and detection actions"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 32, **Halperin** further teaches a method comprising:

A) forming a log to record any predetermined file system operations (Paragraphs 108 and 131).

The examiner notes that **Halperin** teaches **"forming a log to record any predetermined file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108) and "The present invention may be used to identify suspicious activity as it begins to spread within a first group and then receive a report of similar suspicious activity in a second group that is not a neighbor of the first group. In this case, the present invention may be used to analyze recent log files of communications between computing devices in the first and second groups. Since the groups are not neighbors, such communications are not likely to be found under normal circumstances. If a recent communication is identified between the two groups, this may be treated as a suspicious event. The communication may then be forwarded to a human

operator for analysis to identify malicious software. In addition, this process may be used to identify the specific communication message that is carrying the virus, which may lead to containment actions being taken" (Paragraph 131).

Regarding claim 33, **Halperin** further teaches a method comprising:
A) providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"providing means to flag the other program in response to at least one of: the other program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the other program reading or opening itself and the other program attempting to write or append itself or any content to the shared file on the shared or network file system or to write or append itself or any content to the local file on the local file system; the other program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the other program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least

one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 34, **Halperin** further teaches a method comprising:
A) means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"means to flag the other program in response to the other program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior

detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 35, **Halperin** further teaches a method comprising:
A) providing means to send an alert in response to flagging the other program (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"providing means to send an alert in response to flagging the other program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 36, **Halperin** further teaches a method comprising:
A) providing a network monitoring system (Paragraph 111); and
B) providing means to send an alert to the network monitoring system in response to flagging the other program (Paragraph 111)

The examiner notes that **Halperin** teaches **"providing a network monitoring system"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a

suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"providing means to send an alert to the network monitoring system in response to flagging the other program"** as "It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 37, **Halperin** further teaches a method comprising:
A) providing means to present an alert to a user (Paragraphs 73-77); and
B) providing means for the user to approve one of the predetermined file system operations before being performed by the other program (Paragraph 108).

The examiner notes that **Halperin** teaches **"providing means to send an alert in response to flagging the other program"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77). The examiner further notes that **Halperin** teaches **"providing means for the user to approve one of the predetermined file system operations before being performed by the other program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a

system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Regarding claim 38, **Halperin** teaches a computer-readable medium comprising:

A) allowing a security level to be set (Paragraphs 43-44, 108, and 111);

B) monitoring predetermined file system operations associated with a program (Abstract, Paragraphs 73-77, and 88-108); and

C) logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written without performing any virus scanning and detection actions (Paragraphs 108).

The examiner notes that **Halperin** teaches **"allowing a security level to be set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for

messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111). The examiner further notes that **Halperin** teaches **"monitoring predetermined file system operations associated with a program"** "Reference is now made to FIG. 6, which is a simplified flowchart illustration of an exemplary method of operation of the system of FIG. 5, useful in understanding the present invention. In the method of FIG. 6 one or more target behavior profiles are defined for computers 500. Each target behavior profile describes behavior that should be the subject of correlation analysis as described in greater detail hereinbelow. Target behavior may be any and all computer activity. Some examples of target behavior profiles include...Attempting to contact previously unused or unknown IP addresses or IP Sockets" (Paragraphs 88-96), and " Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...A certain percentage of the computers in the network having an unusual level of correlation of data between files sent as attachments. For example, since viruses known as "polymorphic viruses" may change their name as they move from one computer to another, one way to identify such viruses is to identify attachments that have the same or similar data, whether or not they have the same name" (Paragraph 97-106). The examiner further notes that

Halperin teaches **"logging any predetermined file system operations associated with the program including recording a filename and a location where the file is written without performing any virus scanning and detection actions"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 40, **Halperin** further teaches a computer-readable medium comprising:

A) following a predefined procedure in response to the level of security set (Paragraphs 43-44, 108, and 111).

The examiner notes that **Halperin** teaches **"following a predefined procedure in response to the level of security set"** as "In another aspect of the present invention a method for malicious software detection is provided including grouping a plurality of computing devices in a network into at least two

groups, configuring each of the groups to maintain a malicious software detection sensitivity level, and upon detecting suspected malicious software activity within any of the groups, notifying any other of the groups of the detected suspected malicious software activity. In another aspect of the present invention the method further includes adjusting the malicious software detection sensitivity level at any of the notified groups according to a predefined plan" (Paragraphs 43-44), "The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108), and "Alternatively, different systems may have greater or lesser sensitivity levels, or simply different sensitivity levels by employing different sensitivity parameters. Alternatively, each system may use different system decoys and/or monitor different correlation parameters. It is believed that such diversification between different virus containment systems will improve the chances that at least some of the systems will identify a previously unknown virus. Once one system detects a suspected virus it may notify other systems of the suspected virus. Each system may then increase or otherwise adjust its sensitivity level, preferably according to a predefined adjustment plan and preferably in predefined relation to said notification" (Paragraph 111).

Regarding claim 41, **Halperin** further teaches a computer-readable medium comprising:

A) flagging the program in response to the program attempting to perform one of the predetermined file system operations (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to the program attempting to perform one of the predetermined file system operations"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 42, **Halperin** further teaches a computer-readable medium comprising:

A) flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local

file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system (Abstract, Paragraphs 73-77, and 88-108).

The examiner notes that **Halperin** teaches **"flagging the program in response to at least one of: the program opening a local file on a local file system to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file; the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system; the program attempting to write or append the local file to the shared or network file system and preserve a filename of the local file in the shared or network file system; and the program attempting to write or append a remote file to the local file system"** as "A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups, and detecting a change in the value to indicate possible malicious software behavior within the network" (Abstract), "After collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation techniques may be used, such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers...Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as is described hereinabove with reference to FIG. 2" (Paragraph 97-107), and "server 108 may

initiate one or more virus containment actions such as, but not limited to:... Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Regarding claim 43, **Halperin** further teach a computer-readable medium comprising:

A) inhibiting any predetermined file system operations associated with program in response to the program being flagged (Paragraph 108).

The examiner notes that **Halperin** teaches **"inhibiting any predetermined file system operations associated with program in response to the program being flagged"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Regarding claim 44, **Halperin** further teaches a computer-readable medium comprising:

A) sending an alert in response to the program attempting to perform any predetermined file system operations (Paragraphs 73-77).

The examiner notes that **Halperin** teaches **"sending an alert in response to the program attempting to perform any predetermined file system operations"** as "server 108 may initiate one or more virus containment actions such as, but not limited to:...Notifying a user at computer 100 of the suspicious message activity. Notifying a system administrator that a virus may have been detected" (Paragraphs 73-77).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

16. Claims 3-4, 10-11, 20, 22, 31, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Halperin et al.** (U.S. PGPUB 2002/0194490) as applied to claims 1-2, 5, 7-9, 12-19, 21-30, 32-38, and 40-44, in view of **Satterlee et al.** (U.S. PGPUB 2004/0025015).

17, Regarding claim 3, **Halperin** does not explicitly teach a method comprising:

A) monitoring all file operations associated with the program in response to the program not being in a safe list.

Satterlee, however, teaches **"monitoring all file operations associated with the program in response to the program not being in a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 4, **Halperin** does not explicitly teach a method comprising:

A) permitting selected read and write operations in response to a predefined rules table.

Satterlee, however, teaches **"permitting selected read and write operations in response to a predefined rules table"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to

particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 10, **Halperin** does not explicitly teach a method comprising:

A) selecting a program for monitoring in response to the program not being on a safe list.

Satterlee, however, teaches **"selecting a program for monitoring in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 11, **Halperin** further teaches a method comprising:

A) logging any file system operations (Paragraph 108).

The examiner further notes that **Halperin** teaches **"logging any file system operations"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected. The delay period may be set according to different desired levels of system alertness. The delay period may be applied selectively only to certain types of messages, such as those that have attachments or specific types of attachments (e.g., only .exe, .doc, .xls and zip file types). This, too, may be applied selectively according to different desired levels of system alertness. The delay period may also vary for different users, different activities (e.g., such as sending or receiving messages), and/or for messages whose destination is outside of a company or other organization versus internal messages" (Paragraph 108).

Halperin does not explicitly teach:

A) associated with any programs on the safe list.

Satterlee, however, teaches **"associated with any programs on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to

allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 20, **Halperin** further teaches a method comprising:
A) requiring approval before performing any predetermined file system operations associated the program (Paragraph 108).

The examiner notes that **Halperin** teaches **"requiring approval before performing any predetermined file system operations associated the program"** as "In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected message to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be "quarantined" at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations. The server may also notify a system administrator of the quarantined messages who may then check the quarantined to determine whether or not the messages were indeed sent by a computer virus and either allow them to be forwarded to their intended recipients as is, should they not be infected, or only after they have been disinfected" (Paragraph 108).

Halperin does not explicitly teach:
A) in response to the program not being on a safe list.

Satterlee, however, teaches **"in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to

allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 22, **Halperin** does not explicitly teach a system comprising:

A) a safe list; and

B) wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list.

Satterlee, however, teaches **"a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13), and **"wherein the file system program is adapted to monitor the other program in response to the other program not being on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 31, **Halperin** does not explicitly teach a method comprising:

A) providing a safe list; and

B) adapting the file system protection program to monitor the other program in response to the other program not being on the safe list.

Satterlee, however, teaches **"providing a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13), and **"adapting the file system protection program to monitor the other program in response to the other program not being on the safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Regarding claim 39, **Halperin** does not explicitly teach a method comprising:

A) selecting the program for monitoring in response to the program not being on a safe list.

Satterlee, however, teaches **"selecting the program for monitoring in response to the program not being on a safe list"** as "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to particular threats and decision rules as to when the user should be queried about a security threat" (Paragraph 39).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Satterlee's** would have allowed **Halperin's** to provide a method to allow for security systems to enable early detection of threats to a computing device or network before an harm can be done by quickly and efficiently examining code in real time, as noted by **Satterlee** (Paragraph 11).

Response to Arguments

18. Applicant's arguments with respect to claim 1-5, and 7-44 have been considered but are moot in view of the new ground(s) of rejection.

Applicants argue on page 15 that **"Applicants respectfully submit that permitting selected read and write operations in response to a predefined rules table as provided by the embodiment of the present invention as recited in claim 4 is patentably distinct from decision rules as to when a user should be queried about a security threat as taught by Satterlee"**. However, the examiner wishes to point to paragraphs 13 and 39 of **Satterlee** which state "the present invention comprises a method for determining whether a program is approved to execute by comparing it to a predetermined list of approved programs...If the new program is not validated, the program can continue to load and execute, but other security modules are responsible for detecting, monitoring, and responding to suspicious activities" (Paragraph 13) and "predetermined responses to particular threats and decision rules as to when

the user should be queried about a security threat" (Paragraph 39). The examiner wishes to state that **Satterlee's** method clearly allows for some read/write actions to take place from a suspicious program by following predefined rules.

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,886,099 issued to **Smithson et al.** on 26 April 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,735,700 issued to **Flint et al.** on 11 May 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0116639 issued to **Chefalas et al.** on 22 August 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,973,578 issued to **McIchione** on 06 December 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,357,008 issued to **Nachenberg** on 12 March 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0174358 issued to **Wolff et al.** on 21 November 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0015712 issued to **Szor** on 22 January 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0178375 issued to **Whittaker et al.** on 28 November 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2003/0204569 issued to **Andrews** on 30 October 2003. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2005/0268112 issued to **Wang et al.** on 01 December 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0030913 issued to **Liang et al.** on 12 February 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2004/0098607 issued to **Alagna et al.** on 20 May 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 20020194489 issued to **Almogy et al.** on 19 December 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. PGPUB 2002/0188649 issued to **Karim** on 12 December 2002. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,901,519 issued to **Stewart et al.** on 31 May 2005. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 7,093,239 issued to **van der Made** on 15 August 2006. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 5,623,600 issued to **Ji** on 22 April 1997. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 6,763,462 issued to **Marsh** on 13 July 2004. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

U.S. Patent 5,257,381 issued to **Cook** on 26 October 1993. The subject matter disclosed therein is pertinent to that of claims 1-5, and 7-44 (e.g., methods to provide virus protection on computers).

Contact Information

20. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi
Patent Examiner
Art Unit 2168

May 24, 2007

TIM VO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100